How to fairly incentivise digital contact tracing

Loi, Michele

Abstract: Digital apps using Bluetooth to log proximity events (henceforth, digital contact tracing) are increasingly supported by technologists and governments. By and large, the public debate on this matter focuses on privacy, with experts from both law and technology offering very concrete proposals and participating to a lively debate. Far less attention is paid to effective incentives and their fairness. This paper aims to fill this gap by offering a practical, workable solution for a promising incentive, justified by the ethical principles of non-maleficence, beneficence, autonomy and justice. This incentive is a free phone optimised for running such app.

DOI: https://doi.org/10.1136/medethics-2020-106388

How to fairly incentivise digital contact tracing

Michele Loi

Institute of Biomedical Ethics and the History of Medicine and Digital Society Initiative, University of Zurich, Zurich, Switzerland

Correspondence to
Dr Michele Loi, Institute of Biomedical Ethics and the History of Medicine and Digital Society Initiative, University of Zurich, Zurich 8006, Switzerland;
michele.loi@ibme.uzh.ch

Received 1 May 2020
Revised 3 June 2020
Accepted 10 June 2020

ABSTRACT

Digital apps using Bluetooth to log proximity events (henceforth, digital contact tracing) are increasingly supported by technologists and governments. By and large, the public debate on this matter focuses on privacy, with experts from both law and technology offering very concrete proposals and participating to a lively debate. Far less attention is paid to effective incentives and their fairness. This paper aims to fill this gap by offering a practical, workable solution for a promising incentive, justified by the ethical principles of non-maleficence, beneficence, autonomy and justice. This incentive is a free phone optimised for running such app.

INTRODUCTION

The coronavirus disease 2019 (COVID-19) has spread to all continents, contributing to more than ten millions of confirmed cases and a huge amount of deaths in just over 5 months. Governments and health agencies around the world are working together to find solutions to the COVID-19 pandemic, to save lives and to reinvigorate society.

The measures taken to prevent and slow down the spread of the disease include contact tracing, testing and isolation (in some cases involving the prolonged lock-down of entire countries). One goal of governments and health agencies is to enhance the capacity to prevent disease transmission, by tracing and testing, thus reducing the need for the lock-down of entire cities, regions or countries. Health experts and researchers from diverse fields researching disease transmission, including virology, data science and social science, have highlighted the broad variety of information that can be collected, analysed and collected. Some East Asian countries, for example, South Korea, Taiwan and Singapore, have been employing a variety of electronic means to enable contact tracing, such as a public database of known patients, tracking phone location data for anyone under quarantine and tracking when users have been in close proximity via the Bluetooth in their phones.[1]

Digital apps using Bluetooth to log proximity events (henceforth, digital contact tracing) are increasingly supported by technologists[2–4] and governments.[5–8] By and large, the public debate on this matter focuses on privacy risks, with experts from both law and technology offering very concrete proposals to mitigate such risk, which is leading to a lively academic and public debate.[5 6 9–14] Far less attention is paid to the questions of incentives and whether it is possible to have incentives that would be effective and ethical as well. Emerging ethical guideline proposals mention the problem of incentives and access equality[15] and digital inequality more broadly.[16] But no concrete proposal is currently being discussed. This paper aims to fill this gap by offering a practical, workable solution for an incentive that is plausibly effective (section 3) and ethically defensible (section 4). The ethical case for this is built on the ethical principles of non-maleficence, beneficence, autonomy and justice. We start the paper (sections 1 and 2) by briefly presenting the idea of privacy-sensitive contact tracing and the problem of incentives.

Case for privacy-sensitive contact tracing

This paper focuses on one specific class of digital tools against COVID-19, 'proximity tracing tools',[16] designed to enhance the capacity for contact tracing of public health surveillance systems. The Singapore app, for example, allows the Ministry of Health to determine the first-degree contacts of anyone logged by Bluetooth to be near them, which enhances the capacities of human contact tracers to follow up on those contacts with appropriate measures.[11] In parallel, Apple and Google have enabled a decentralised contact tracing capacity on their phones, which will enable a more efficient logging of nearby contacts by using the Bluetooth technology on iOS and Android phones.[17] Proximity tracing tools should be distinguished from other types of digital tracing tools, in particular symptom checkers, quarantine compliance tools and flow modelling tools.[16 18]

One reason for the focus in this paper is that digital proximity tracing tools are seen as especially valuable complements to analogue contact tracing. Manual contact tracing does not scale easily,[19] it is slow (an estimated average time of 12 hours to trace the contacts of a single infected individual),[13] subject to memory gaps and is arguably more privacy invasive, as connections between reported and suspected cases shall be made clear to health officials. Yet this interference with privacy is widely regarded as justified[20] because contact tracing advances public health goals, facilitating a step-by-step return to an open society and economy. This can only happen if health systems are not overwhelmed, as seen, for example, in the Italian region of Lombardy.[21] This requires effective containment of the disease. While digital contact tracing also impinges on privacy by requiring some kind of access to health status and behaviour, the privacy risks vary depending on the data types and protocols used by such tools.

It has been argued that Bluetooth proximity tracing in particular can be achieved collecting a minimal amount of data. Consider for example the TraceTogether app in Singapore: tracing works by producing ephemeral tokens (time-varying random strings) that are exchanged between different devices when these remain sufficiently near for a sufficient length of time. A proximity event is thus registered through such Bluetooth 'handshakes'. When an individual is diagnosed with COVID-19,

To cite: Loi M. *J Med Ethics* Epub ahead of print: [please include Day Month Year]. doi:10.1136/medethics-2020-106388

all pseudonymised tokens in a defined time period (eg, 14 days) are released and made public by an authority—typically a government server. Since the tokens are pseudonymous, the app user has no way to identify whom the tokens stored in their app belong to. But when a list of tokens is made public, the authority has a way to send alerts to the people who have been in close proximity to it.

Notice that there are at least two very different ways of doing this: the Singapore app is referred to as *centralised* because each phone sends a list of all the tokens of *other* phones with which it has shaken hands. When one person is reported as infected, the authority is able to contact the owners of other phones directly. This approach relies on trust in the government authority to respect the privacy of individuals.[1] By contrast, in decentralised approaches, the phone of the infected individual does not share with the authority the tokens of all its handshakes. Rather, it uploads only the list of the tokens *it has generated* and let the apps in other phones check whether a handshake has taken place. The central authority has no way to reach or communicate with the proximate, not yet clinically tested, individuals, for it holds no data, not even pseudonymised ephemeral tokens, generated by their devices. This is roughly speaking the difference between the two approaches.[19][i] In this paper, this contentious issue is sidestepped completely. Notice that, *in both* approaches, only pseudonymised ephemeral tokens are uploaded in central servers.

It has to be highlighted that while Bluetooth tools do not record position data (mitigating location-based group stigmatisation, eg, based on place of worship), all contact tracing protocols threaten privacy to a certain extent. The decentralised approach shares at least part of the social graph around an infected individual with authorities, empowering sufficiently motivated government officials and hackers to de-anonymise these data. Even in decentralised approaches, sufficiently motivated attackers (including state officials) can perform re-identification attacks on high-value individuals, groups or geographical areas[22] (arguably, however, such attacks are not likely to scale to the level of mass surveillance). The likelihood of such scenarios is highly debated in the expert community.[23] In what follows, we shall assume that risks for privacy are low in both cases, at least if additional social and legal safeguards are in place. Examples of such safeguards are human rights laws, an independent judiciary, laws protecting journalists and whistleblowers, sunset clauses and laws mitigating the risk of forced choice, for example, punishing individuals in a position of power if they demand the installation of the apps by people subjected to it.[ii]

Summing up, digital contact tracing is seen as a more efficient[24] and (at least in the Bluetooth implementation) more privacy-preserving alternative than any existing alternative for contact tracing. In the light of this, it is not surprising to see that many government-backed and independent initiatives such as NHSX, PEPP-PD, DP-3T and ROBERT have started defining technological standards to realise a Bluetooth solution enabling digital contact tracing.[iii] While perfect security and privacy are not achievable, many people can consider such apps to provide acceptable protections, and this can be regarded entirely reasonable.

Voluntariness and incentives

Let us assume that the app guarantees to most people a sufficient degree of privacy protection given its purpose. In order to fulfil its public health use, any such app should be used by a considerable proportion of the population.[iv] In spite of that, most countries have decided that the app should be adopted *voluntarily*. In Singapore, one of the most technologically advanced and richest nations in the world, only about 17% of the population downloaded the app.[25] Thus, it is plausible to think that a voluntary app needs, beside strong privacy and security guarantees, some kind of incentive in order to be adopted. As noted by Floridi,[26] many incentives generate unfairness. If you attach a benefit to having or using the app (eg, you must have the app to enter public buildings and transportation), you confer a benefit to that segment of the population who owns and can use smartphones already. Even in Europe, one of the richest, most highly educated and technologically advanced areas of the world, significant inequalities in digital skills exist and 17% of the population has no digital skills (defined as people who do not use the internet or only seldomly do so).[27] So, incentives of that type raise issues of fairness and social justice.[v]

Proposal of fair incentives

This proposal is to incentivise the app by fully subsidising a smartphone with the preinstalled digital tracing app, requiring a single click to activate it, after completing the informed consent procedure (which should also be possible with a human operator, by phone). The phone should be optimised for use by the individuals with no digital skills. High usability is required to mitigate, to the greatest possible extent, difficulties due to the lack of digital skills of the user. This would require careful design and empirical testing. Conceivably, optimising usability for people lacking digital skills may lead to sacrificing most smart functions beside phone calls and running the contact tracing app in the background. (Visually, such device may end up looking like a replica of some early 2000s phone.) The phone should perhaps have a very clear indication of its additional (smart) function, which distinguishes from other older-looking phones; for example, it must be branded 'digital tracing Covid' and be easily recognisable as such. There are two reasons for this: to make sure that the user is aware that the phone provided for free is not just any ordinary phone, and to signal this to others. The ability to signal tracing to others is a safeguard *for the user* in a scenario

[i] Roughly speaking, because one can distinguish two types of centralised approaches: one in which only the infected person uploads its list of contacts, and one in which all do. This difference between the former centralised protocol and the decentralised one is the difference between protocol 2 and protocol 3 in.[30] The Apple/Google protocol follows the decentralised approach.[17]

[ii] Example of such legal provisions are found in.[6 12]

[iii] See[31] for a fuller list. Notice that not all initiatives worldwide are considering Bluetooth, eg, MIT Safe Paths uses GPS.

[iv] 60% adoption rate has been widely discussed as an estimate. The figure is a gross oversimplication of the model presented in.[24] To see why, consider that the model includes several assumptions about disease transmission and a chance in such assumptions—that are far from certain—implies a change in this estimate.

[v] There are other objections against incentives, beside fairness. For example, linking the possibility to enter the metro or go to certain places to a notification of being 'free from contagion' generates an incentive for the individual not to carry their phone whenever they can avoid it, which compromises data quality. When return to social life is conditioned on using the app, there will be also a problem in the legal grounds of data processing since "consent given to the processing of data acquired via the mechanisms described so far could not be regarded as valid if it were framed as a precondition, for instance, to obtain certain services or goods—as was the case in China".[32]

in which digitally competent individuals exclude or stigmatise non-app-users and citizens using old phones are simply assumed to be non-app users. Immediately after the first initialisation of the operating system, the user should be asked to provide his or her informed consent to using the (already installed) contact tracing app. The informed consent form should explain the function of the digital contact tracing app, data processing and economic conditions in the simplest possible way. The user must have a clear opportunity to decline consent, but, in that case, a procedure will be activated, which will imply the restitution of the subsidy received by the state to obtain the phone. This is needed to prevent an inefficient use of state funds: the phone is for the people who are at least *initially motivated* to contribute to contact tracing. One month after the activation, the user should be free to uninstall the app phone without any financial penalty and should be made aware of this opportunity (this will be justified when discussing the value of autonomy).

Ethical assessment of the proposal

In this section, it is shown that the proposal is ethically justified, appealing to the bioethical principles of *non-maleficience*, *beneficence*, *autonomy* and *justice*.

Non-maleficence

The proposal is ethically justified by non-maleficence, *a fortiori*, by the same arguments that make a *compulsory* app *prima facie* ethically justified by non-maleficence.[28] When a person has the possibility to mitigate serious risks to others, at little cost for him or herself, she is arguably morally required to do that. A person who is potentially contagious puts the lives and health of people near her at risk. A person who has no information about her past proximity to infected individuals also poses a significant risk to others, as the spread of the disease through asymptomatic individuals has shown. This risk can be reduced by using the app and self-isolating when one receives a notification of a proximity event. Compared with the threat posed to public health, the burden for the user of the app is small, if a clinical test (eg, swab tests) is offered swiftly to the person receiving the notification (to exclude a false positive) and other measures (eg, health insurance and unemployment benefits, covering absence from or inability to work) are in place.

From the point of view of non-maleficence, a voluntary app endorsed by a large proportion of the population (eg, 60%) is preferable to one that is compulsory, even if the latter is used more widely. The compulsory use of a portable device is either poorly enforced or enforced in a way that only an authoritarian regime would be willing to implement. A voluntary app is also fail-safe against government abuse and a higher-than-expected frequency of hacker attacks: if privacy violations and data misuse scandals emerge, a critical citizen may simply uninstall the app or stop using the COVID-19 phone.

Beneficence

The incentive proposal is *prima facie* justified from the point of view of beneficence since it pursues a public health purpose of primary importance. Public health encompasses the absence of disease and all the benefits deriving from the fact that individuals can return to a normal life and avoid conditions of economic deprivation. Beneficence only supports *effective* digital contact tracing, and an incentive system is a means to achieve widespread voluntary adoption, which makes digital contact tracing effective. The proposal is arguably a good incentive since people are generally attracted to free gadgets. The scheme is relatively efficient because prospective free riders are at least induced to use the app for 1 month, and possibly sceptical or prejudged users are initially attracted to use it (by the selfish motivation to obtain a free phone) and given enough time to reflect carefully before uninstalling the app.

Autonomy

Nobody is obliged to use the smartphone, so user autonomy is respected. If coercive social norms to use such apps emerge, these phones can even be used—after 1 month—to mislead the observers about one's user status and avoid social pressures: people may use a 'fight COVID' branded phone after uninstalling the app. Users who change their minds about the risks of digital contact tracing can simply uninstall the app (without penalties after the first month) or purchase a new phone. It may be objected that offering a phone for free amounts to a coercive offer.[29] But an elementary phone, optimised for ease of use by unsophisticated users, with a branding associated with COVID-19, that everyone can get for free, does not have a very high use value, market value or status symbol value (eg, compared with a high-end phone). While the phone is meant to be attractive, it is certainly not so attractive to be considered 'an offer one cannot refuse'.

Justice

Unlike incentives directed to people who *already* possess and can use a smartphone, this incentive is especially fair. The phone should be optimised to promote acceptance and usability by those citizens who currently do not use internet-capable phones or do not use their phones to access the internet (even when their phones are internet capable). The difficulties associated with the lack of digital skills may be more cognitive and generational than economic. A phone optimised in this way is unlikely to attract people with high digital skills. The subsidy provided by the rest of society naturally reaches the group that is worst off in the most relevant sense, in this context. This type of self-selection is preferable to means testing because it avoids bureaucratic frictions and also because the most relevant needs derive from a lack of digital competences, not a lack of purchasing power. (Many individuals otherwise excluded from contact tracing, namely older people, may not be among the poorest in society in wealth terms, eg, they may own a house.) The phone would be no status symbol or high-tech gadget benefiting the already well off.

CONCLUSION

Digital contact tracing apps with low adoption rates have little value for public health and their users because they are ineffective. One risk is that such apps will never be used by a segment of the population lacking digital skills. Some potentially effective incentives to use digital tracing apps are unfair, coercive and do not favour the inclusion of this group. Here, we offer a potential solution: a psychological and economic incentive (a free phone) that is neither coercive nor unfair.

Acknowledgements The author wishes to thank Paul O Dehaye and PersonalData.IO for insightful discussions on this topic.

Contributors I am the sole author and sole contributor to this paper.

Funding The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.

Competing interests ML reports personal fees from Health-Catalyst, outside the submitted work.

Patient consent for publication Not required.

Provenance and peer review Not commissioned; externally peer reviewed.

Data availability statement There are no data in this work.

ORCID iD
Michele Loi http://orcid.org/0000-0002-7053-4724

REFERENCES

1 Cho H, Ippolito D, Yu YW. "Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs," *ArXiv200311511 Cs*, 2020. Available: http://arxiv.org/abs/2003.11511 [Accessed 30 Apr 2020].
2 "Watch." Covid. Available: https://www.covid-watch.org [Accessed 30 Apr 2020].
3 "DP-3T/documents," *GitHub*. Available: https://github.com/DP-3T/documents [Accessed 30 Apr 2020].
4 "PEPP-PT," Pepp Pt. Available: https://www.pepp-pt.org [Accessed 30 Apr 2020].
5 NHSX, "The power of data in a pandemic." /blogs/power-data-pandemic/ [Accessed 30 Apr 2020].
6 "App Immuni, il governo detta le regole: nessuna conseguenza se si decide di non usarla," *la Repubblica*, 2020. Available: https://www.repubblica.it/politica/2020/04/30/news/cdm_governo_app_immuni_giustizia_scarcerazioni-255224818/ [Accessed 30 Apr 2020].
7 Dillet R. "France is officially working on 'Stop Covid' contact-tracing app | TechCrunch". Available: https://techcrunch.com/2020/04/08/france-is-officially-working-on-stop-covid-contact-tracing-app/ [Accessed 30 Apr 2020].
8 "Germany's COVID-19 contacts tracing app to link to labs for test result notification," TechCrunch. Available: https://social.techcrunch.com/2020/04/23/germanys-covid-19-contacts-tracing-app-to-link-to-labs-for-test-result-notification/ [Accessed 30 Apr 2020].
9 European Data Protection Board, "Statement on the processing of personal data in the context of the COVID-19 outbreak", 2020. Available: https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf
10 Contact tracing in the real world | Light Blue Touchpaper. Available: https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/ [Accessed 26 Apr 2020].
11 Help speed up contact tracing with TraceTogether. Available: http://www.gov.sg/article/help-speed-up-contact-tracing-with-tracetogether [Accessed 30 Apr 2020].
12 Edwards L*et al*. The coronavirus (safeguards) bill 2020: proposed protections for digital interventions and in relation to immunity certificates. *LawArXiv, preprint* 2020.
13 European Centre for Disease Prevention and Control,. "Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union—second update," European Centre for Disease Prevention and Control, 2020. Available: https://www.ecdc.europa.eu/en/covid-19-contact-tracing-public-health-management [Accessed 30 Apr 2020].
14 European Commission, "Guidance on apps supporting the fight against COVID 19 pandemic in relation to data protection," European Commission, C(2020) 2523 final, 2020. Available: https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf
15 Morley J, Cowls J, Taddeo M, *et al*. *Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems, Social Science Research Network*. Rochester, NY: SSRN Scholarly Paper ID 3582550, 2020. https://papers.ssrn.com/abstract=3582550
16 Gasser U, Ienca M, Scheibner J, *et al*. "Digital tools against COVID-19: framing the ethical challenges and how to address them," *ArXiv200410236 Cs*, 2020. Available: http://arxiv.org/abs/2004.10236 [Accessed 30 Apr 2020].
17 Apple and Google, "Privacy-Preserving Contact Tracing," *Apple*. Available: https://www.apple.com/covid19/contacttracing [Accessed 30 Apr 2020].
18 Ienca M, Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic. *Nat Med* 2020;26(4):463–4.
19 Salathe M, Cattuto C. "Covid19-response. What data is necessary for digital proximity tracing".
20 World Health Organization. *WHO Guidelines on Ethical Issues in Public Health Surveillance*. Geneva: WHO, 2017.
21 Odone A, Delmonte D, Scognamiglio T, *et al*. COVID-19 deaths in Lombardy, Italy: data in context. *Lancet Public Health* 2020;5(6).
22 The DP-3T project, "Privacy and Security Attacks on Digital Proximity Tracing Systems," GitHub, Apr. 21, 2020. Security analysis/Privacy and Security Attacks on Digital Proximity Tracing Systems.pdf.
23 "Risk of de-anonymization of infected users is much higher than estimated · Issue #169 · DP-3T/documents," GitHub. Available: https://github.com/DP-3T/documents/issues/169 [Accessed 1 Jun 2020].
24 Ferretti L, Wymant C, Kendall M, *et al*. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 2020;368(6491):eabb6936.
25 Chong C. About 1 million people have downloaded TraceTogether app, but more need to do so for it to be effective: Lawrence Wong. *The Straits Times* 2020.
26 Floridi L. "Mind the app—considerations on the ethical risks of COVID-19 apps". Available: https://thephilosophyofinformation.blogspot.com/2020/04/mind-app-considerations-on-ethical.html [Accessed 30 Apr 2020].
27 Digital Skills and Jobs Coalition of the European Union, Human Capital Digital Inclusion and Skills. Available: https://ec.europa.eu/information_society/newsroom/image/document/2018-20/2_desi_report_humancapital_B5DC055D-DD1E-51CD-229138BE55F9AE8A_52247.pdf
28 Canca C. "Why 'Mandatory Privacy-Preserving Digital Contact Tracing' is the Ethical Measure against COVID-19," *Medium*, 2020. Available: https://medium.com/@cansucanca/why-mandatory-privacy-preserving-digital-contact-tracing-is-the-ethical-measure-against-covid-19-a0d143b7c3b6 [Accessed 30 Apr 2020].
29 O'Neill O. Some limits of informed consent. *J Med Ethics* 2003;29(1):4–7.
30 de Montjoye Y-A, Houssiau F, Gadotti A, *et al*. "Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask.". Available: https://cpg.doc.ic.ac.uk/blog/evaluating-contact-tracing-apps-here-are-8-privacy-questions-we-think-you-should-ask/ [Accessed 30 Apr 2020].
31 eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States, 2020. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf
32 Antonello S. "Audizione informale, in videoconferenza, del Presidente del Garante per.—Garante Privacy,", 2020. Available: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9308774 [Accessed 30 Apr 2020].